

matrix:

.....
.....001010101110101.....
.....011110111010101...
.....101011101110101.....
.....011010101000111...
.....101010100110101....
.....

33. A method for creating an encryption key, comprising:

creating a set of vertices, each vertex in the set of vertices being associated with a symbol from a first set of symbols; and

defining a relationship for pairs of vertices in the set of vertices, wherein for each pair the relationship is expressed by a vector originating in one vertex and terminating in another vertex, the vector being associated with a symbol from a second set of symbols. --

REMARKS

Favorable reconsideration of the present application is respectfully requested in view of the foregoing amendments and the following remarks. Claims 1, 7-10, and 16 have been amended, claims 6 and 14-15 have been canceled, and claims 17-33 have been added. Applicant submits that no new matter has been added. Claims 1-5, 7-13, and 16-33 are pending after the instant amendments.

Lack of Enablement Rejection under 35 U.S.C. §112, first paragraph

The Examiner rejected claim 14 under 35 U.S.C. §112, first paragraph, for containing subject matter which was not described in the specification in such a way as to enable one skilled in the art to make and/or use the invention. The rejection of claim 14 is now moot in light of its cancellation.

Indefiniteness Rejections under 35 U.S.C. §112, second paragraph

In the Office Action, the Examiner rejected claims 7, 8, 11, 12, 15, and 16 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the invention. Applicant respectfully traverses the rejection of claims 7 and 8 for lack of antecedent basis because those claims have been amended to depend from claim 2, and claim 2 introduces the “second key” element referred to in claims 7 and 8. Claim 2 thus provides antecedent basis for the term “the second key” as it appears in claims 7 and 8. Therefore, the rejection of claims 7 and 8 should be withdrawn. Further, because claims 11 and 12 depend from claim 7, and claim 7 as amended complies with the requirements of 35 U.S.C. §112, second paragraph, the indefiniteness rejection of claims 11 and 12 should also be withdrawn.

The rejection of claim 15 is now moot in light of its cancellation.

The Examiner asserted in the Office Action that the term “large number” renders claim 16 indefinite. Because that term has been deleted from the claim, Applicant submits the rejection of claim 16 should be withdrawn.

Anticipation Rejections under 35 U.S.C. §102

The Examiner rejected claims 1-16 under 35 U.S.C. §102(a,b) as being clearly anticipated by the article titled Leonardo/Daniel. In response to the Examiner’s request to the Applicant to

clarify the authorship and publication date of the article, Applicant submits that he is the author of the article and that the article was published on March 25, 1999. Consequently, the reference should not be used as prior art and the rejections based on this reference should be withdrawn.

The Examiner rejected claims 1, 4, 6, 7, 9-13 and 15-16 under 35 U.S.C. §102(b) as being clearly anticipated by Gaines (Reference R, 1939). The Examiner also rejected claims 1, 4, 7, 9-13, and 15-16 under 35 U.S.C. §102(b) as being clearly anticipated by Manual of Cryptography (Reference S).

Regarding the rejection of claim 1 as being clearly anticipated by Gaines, the Examiner asserted that Gaines' invention "inserts nulls between all repeating letters to make a non-repeating plaintext", which "makes the ciphertext a different size from the plaintext." Gaines, however, does not disclose (a) "converting the plaintext into a sequence of symbols with a 1:n relationship, wherein n is an integer greater than 2" and (b) "converting the sequence of symbols into a non-repeat sequence of symbols" as required by claim 1 of the present invention, because inserting nulls between all repeating letters in the plaintext clearly differs from converting the plaintext to a sequence of symbols. Even if the Examiner reads Gaines as showing the conversion of plaintext into a sequence of symbols, that conversion does not follow a 1:n relation as is recited in claim 1.

The Manual of Cryptography ("the Manual") also fails to disclose elements (a) and (b) from claim 1. The Examiner asserted that the Manual inherently discloses the use of an intervening letter between any doubles. That falls short of showing a conversion of plaintext into a sequence of symbols and then converting that sequence of symbols into a non-repeat sequence. For the foregoing reasons, neither the Manual nor Gaines disclose each and every element of

claim 1 and thus neither reference anticipates claim 1. Therefore claim 1 should be allowed.

The Examiner is reminded that the MPEP requires that the Examiner use only the best prior art available. For Example, the Examiner should use a single reference (either the Manual or Gaines) in rejecting a given claim (e.g., claim 1) under anticipation grounds.

Claims 2-5, 7-13, and 16 should be allowed at least by virtue of their dependency from claim 1.

Obviousness Rejections under 35 U.S.C. §103(a)

The Examiner rejected claims 1, 2, 4, 5, and 8 under 35 U.S.C. §103(a) as being unpatentable over Schneier. The Examiner states that the reference teaches a method of generating a ciphertext which will decrypt to two different messages under two different keys. The Examiner noticed that the reference does not teach transforming the plaintext into non-repeating plaintext, but asserts that it is well known in the art to add in additional characters in the plaintext to help break up the natural building blocks of the plaintext language so that decryption is complicated. Applicant respectfully disagrees with the Examiner's statement and requests that the Examiner provide a reference that discloses what he asserts to be well known in the art. Most important, Applicant submits that a person of ordinary skill would not have been motivated to combine the teachings of Schneier with the technique of transforming plaintext into non-repeating plaintext to complicate decryption, because the complexity of the decryption process lies in the randomness of the encryption key and not in the pattern of the plaintext. For the foregoing reasons, Schneier does not render obvious claims 1, 2, 4, 5, and 8 and such claims should therefore be allowed.

New claims 17-33 and Examiner's Interview

New claims 17-33 have been added to more accurately define the invention. In the Examiner's Interview the Examiner agreed that the "actual" or present invention disclosed differs from the prior art cited, as noted in the Interview Summary. Because the new set of claims 17-33 define the invention as it was discussed with the Examiner during the interview, the new claims represent the "actual" invention and thus they are not taught by the cited prior art. Therefore, Applicant submits that the new claims are in condition for allowance.

As all grounds of objection and rejection have been addressed and overcome, entry of this Amendment and issuance of a Notice of Allowance of the claims now presented, are respectfully solicited.

In the event there are any questions relating to this Amendment or the application in general, it would be appreciated if the Examiner would telephone the undersigned attorney concerning such questions so that prosecution of this application may be expedited. Please charge any shortage or credit any overpayment of fees to Deposit Account No. 23-2185.

In the event that a petition for an extension of time is required to be submitted herewith and in the event that a separate petition does not accompany this response, Applicant hereby

petitions under 37 CFR 1.136(a) for an extension of time for as many months as are required to render this submission timely. Any fee due is authorized above.

Respectfully Submitted,

BLANK ROME COMISKY & MCCAULEY LLP

By: 

Michael C. Greenbaum
Reg. No. 28,419

The Farragut Building
900 - 17th Street, N.W., Ste. 1000
Washington, D.C. 20006
Telephone: (202) 530-7400
Facsimile: (202) 463-6915

Date: November 1, 2000